a.) Amendments to Specification

Replace the paragraph beginning at page 1, line 14, in the specification as originally filed, with the following rewritten paragraph:

--With advances in integrated circuit, microprocessor, networking and communication technologies, increasing numbers of devices, in particular, digital computing devices, are being networked together. Devices are often first coupled to a local area network, such as an Ethernet based office/home network. In turn, the local area networks are interconnected together through wide area networks, such as ATM networks, Frame Relays, and the like. Of particular ~~notoriety~~ interest is the TCP/IP based global inter-networks, Internet.--

Replace the paragraph beginning at page 1, line 21, in the specification as originally filed, with the following rewritten paragraph:

--As a result of this trend of increased connectivity, increasing numbers of applications that are network dependent are being deployed. Examples of these network dependent applications include but are not limited to, email, net based telephony, world wide web and various types of e-commerce. Success of many of these content/service providers as well as commerce sites depends on the quality of service that they provide.--

Replace the paragraph beginning at page 2, line 9, in the specification as originally filed, with the following rewritten paragraph:

--To[-] date, all the known methods and apparatuses that can assist a system owner in protecting his/her systems from being exploited are basically intrusion protection oriented. That is all the methods and apparatuses are substantially oriented towards keeping undesirable network traffics from entering a network domain and/or preventing unauthorized program ~~executing~~ execution on the owner's systems. As experience ~~have~~ has demonstrated, none of these methods and apparatuses is perfect. From time to time, we have learned that hackers are able to get through. Thus, additional methods and apparatuses that can further prevent systems from being exploited ~~in~~ and giving involuntary assistance to DOS attacks are desired.--

Replace the paragraph beginning at page 2, line 22, in the specification as originally filed, with the following rewritten paragraph:

--The present invention provides for a novel approach to warning and/or protecting a system owner's system(s) from being exploited in providing involuntary assistance to a DOS attack. The present invention provides the protection by detecting and/or preventing undesirable or inappropriate network traffic from being sourced from a network domain. More specifically, a monitor/regulator is provided to monitor network traffic leaving a network domain. The monitor/regulator determines if undesirable/inappropriate network traffics are leaving the network domain based on the observed characteristics of the outbound and inbound network traffics. In one embodiment, if it is determined that undesirable/inappropriate network traffics are leaving the network domain, the monitors/regulator at least issues warnings, alerting system owners of the detection. In another embodiment, the monitor/regulator further issues regulation instruction(s) to boundary routing device(s) of the network domain(s), thereby preventing the network domain(s) from being exploited to source such undesirable/inappropriate network traffics.--

Replace the paragraph beginning at page 4, line 15, in the specification as originally filed, with the following rewritten paragraph:

--Figures 3a-3c illustrate the present invention in further details, in accordance with three embodiments; and--

Replace the paragraph beginning at page 5, line 6, in the specification as originally filed, with the following rewritten paragraph:

--Parts of the description will be presented in terms of operations performed by a processor based device, using terms such as receiving, analyzing, determining, instructing, and the like, consistent with the manner commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. As well understood by those skilled in the art, the quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, and otherwise manipulated through mechanical and electrical components of the processor based device; and the term processor includes microprocessors, micro-controllers, digital signal processors, and the like, that are standalone, adjunct or embedded.--

Replace the paragraph beginning at page 5, line 16, in the specification as originally filed, with the following rewritten paragraph:

-- Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, ~~however~~ but, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations need not be performed in the order of presentation. The terms "routing devices" and "route" are used throughout this application, in the claims as well as in the specification. The terms as used herein are intended to be genus terms that include the conventional routers and conventional routing, as well as all other variations of network trafficking, such as, switches or switching, gateways, hubs and the like. Thus, unless particularized, the terms are to be given this broader meaning. Further, the description repeatedly uses the phrase "in one embodiment", which ordinarily does not refer to the same embodiment, although it may.--

Replace the paragraph beginning at page 7, line 6, in the specification as originally filed, with the following rewritten paragraph:

-- Figure 3a illustrates a first embodiment of the present invention, wherein network domain 104' has a single egress point for network traffics 106 to leave network domain 104' and enters internetworking fabric 108. As described earlier, monitor/regulator 102' monitors or observes network traffics 106' routed between network domain 104' and internetworking fabric 108 through routing device 114' (block 202), and based on observations 110', determines if undesirable or inappropriate network traffics are being sourced out of network domain 104' into internetworking fabric 108 through routing device 114' (block 204). If so, for one implementation of the illustrated embodiment, monitor/regulator 102' at least issues warnings alerting system owners of the detection. In another implementation, monitor/regulator 102' regulates routing device 114', issuing regulation instructions 112' to routing device 114' to "stop" routing certain traffic, to prevent the undesirable or inappropriate network traffics from being sourced out of network domain 104 into internetworking fabric 108 through routing device 114' (block 206). As a result, systems disposed inside network domain 104' are warned

and/or protected from exploitation in providing involuntary assistance to DOS attacks against other systems.--

Replace the paragraph beginning at page 7, line 23, in the specification as originally filed, with the following rewritten paragraph:

-- In one embodiment, routing device 114' is of a type equipped to provide aggregate characteristic statistics on network traffics 106' routed. Examples of these aggregate characteristic statistics include but are not limited to statistics for traffics of particular types routed in both the outbound and inbound directions. [Outbound refers to network traffics routed from network domain 104' onto internetworking fabric 108', and inbound refers to the opposite.] Other examples of aggregate statistics include the number of bits per second (mbps), the number of packets per second, or the number of flows per second routed in each direction. [A flow may e.g. be a unique traffic conversation as indicated by a combination of source and destination addresses (and for certain protocols, port number also).] Further, the aggregate statistics may also include volume of data destined for specific destination addresses, lengths of packets, distribution of Time To Live values, and so forth. These other aggregated characteristic statistics may also be provided by network traffic type. In other words, aggregate characteristic statistics may simply be whatever data are necessary to provide the desired level of granularity in discerning undesirable versus desirable or appropriate versus inappropriate network traffics.--

Replace the paragraph beginning at page 9, line 1, in the specification as originally filed, with the following rewritten paragraph:

--Numerous routing devices with such data providing capability are known in the art, including but are not limited to routing devices available from CISCO Systems, or 3COM, both of San Jose, CA, or Juniper Networks of Sunnyvale, CA.--

Replace the paragraph beginning at page 9, line 24, in the specification as originally filed, with the following rewritten paragraph:

--In one embodiment, monitor/regulator 102' makes the determination based at least on the relative difference between the number of outbound TCP SYN and FIN packets and the number of inbound response packets responding to these packets.

Monitor/regulator 102' infers that undesirable/inappropriate traffics are being sourced out of network domain 104' if the difference exceeds a predetermined threshold. The predetermined threshold is empirically determined, and typically set at a relatively high level. If notwithstanding the relatively high level, the threshold is still exceeded, the excess suggests that the target destinations of the TCP SYN and FIN packets may be unable to respond due to a deliberate concentration of network traffic targeting one or more destinations. Accordingly a high likelihood exists then, a substantial amount of these TCP SYN and FIN packets are associated with a DOS attack.--

Replace the paragraph beginning at page 10, line 10, in the specification as originally filed, with the following rewritten paragraph:

-- In one embodiment, monitor/regulator 102' additionally or alternatively makes the determination based on the relative difference between the number of outbound TCP SYN and FIN packets destined for certain destinations, and the number of follow-on non-TCP SYN and FIN packets to the same destinations (typically representative of subsequent substantive requests from a destination after the initial connections established via the TCP SYN and FIN packets). Monitor/regulator 102' infers that undesirable/inappropriate traffics are being sourced out of network domain 104' if the difference exceeds a predetermined threshold. The predetermined threshold is also empirically determined. If the threshold is exceeded, the lack of follow-on substantive non-TCP SYN and FIN packets suggests that the target destinations of the TCP SYN and FIN packets may be just contacted to clog up the destinations. Accordingly, a high likelihood exists ~~then~~ that, a substantial amount of these TCP SYN and FIN packets are associated with a DOS attack.--

Replace the paragraph beginning at page 12, line 16, in the specification as originally filed, with the following rewritten paragraph:

-- In any event, if monitor/regulator 102' concludes that undesirable/inappropriate network traffics are not being sourced out of network domain 104', monitor/regulator 102' takes no further action. On the other hand, if monitor/regulator 102' concludes that undesirable/inappropriate network traffics are being sourced out network domain 104', in one embodiment, monitor/regulator 102' issues at least warnings alerting system owners

of the detections. The warnings may be delivered in any one of a number of form factors, including electronic messages (delivered e.g. to control consoles, pagers and the like), faxes, audio messages, and the like. For the illustrated embodiment, monitor/regulator 102' further instructs routing device 114' to regulate the manner in which routing device 114' routes traffics 106' onto internetworking fabric 108, to attempt to "stop" these undesirable/inappropriate traffics from being sourced out of network domain 104'.--

Replace the paragraph beginning at page 13, line 3, in the specification as originally filed, with the following rewritten paragraph:

--For examples, monitor/regulator 102' may instruct routing device 114' to drop certain types of packets, or packets destined for certain destinations. Alternatively, monitor/regulator 102' may instruct routing device 114' to lower the routing priority of these packets or limiting the amount of bandwidth being given for these packets, thereby slowing the rate or reducing the volume of these packets from being sourced out of network domain 104'. As a result, monitor/regulator 102' effectively "stops" the undesirable/inappropriate network traffics from being sourced out of network domain 104'. In one embodiment, monitor/regulator 102' uses interface related commands such as "show interface rate-limit" and "rate-limit" to regulate and de-regulate routing device 114'. The functions and constitutions of these commands are also known in the art, accordingly will not be further described.--

Replace the paragraph beginning at page 14, line 11, in the specification as originally filed, with the following rewritten paragraph:

-- Similarly, when monitor/regulator 102'' makes its determination on whether undesirable/inappropriate network traffics are being sourced out of network domain 104", monitor/regulator 102'' takes all the data received into consideration. That is, when analyzing the data received from routing device 114"a, monitor/regulator 102'' adds or otherwise factors into consideration the data received from routing device 114"b. Similarly, when analyzing the data received from routing device 114"b, monitor/regulator 102'' adds or otherwise factors into consideration the data received from routing device 114"a. As described earlier, the data may be any one of the example data enumerated above, aggregated or at individual flow level.--

Replace the paragraph beginning at page 14, line 20, in the specification as originally filed, with the following rewritten paragraph:

-- By aggregating or otherwise ~~takes~~ taking into consideration characteristic data of network traffics sourced out of routing device 114"a as well as routing device 114"b, monitor/regulator 102" is made more sensitive[,] and ~~be~~ able to detect undesirable/inappropriate network traffics being sourced out of network domain 104", even though the decision metrics may not be exceeded at the individual boundary routing devices 114"a and/or 114"b.--

Replace the paragraph beginning at page 15, line 9, in the specification as originally filed, with the following rewritten paragraph:

-- As alluded to earlier, while for ease of understanding, monitor/regulator 102'' is shown as externally disposed away from routing devices 114"a and 114"b, the present invention may be practiced with monitor/regulator 102'' implemented as a standalone component, independently and externally disposed away from routing device 114', or alternatively, the present invention may be practiced with monitor/regulator 102'' distributively, with at least a part of monitor/regulator 102" integrally implemented as a part of routing device 114"a and/or routing device 114"b, as long as the distributed pieces are communicatively coupled to each other and ~~be~~ are able to cooperatively practice the present invention.--

Replace the paragraph beginning at page 15, line 20, in the specification as originally filed, with the following rewritten paragraph:

--Figure 3c illustrates a third embodiment of the present invention, wherein monitor/regulator 102"' monitors and regulates network traffics sourced out of multiple network domains, e.g. network domains 104"'a as well as network domains 104"'b. Each network domain 104"'a/104"'b has one or more egress points for network traffics 106"' to leave the particular network domains 104"'a/104"'b, and enters internetworking fabric 108. As described earlier, monitor/regulator 102"' monitors network traffics 106"', determines if undesirable/inappropriate network traffics are being sourced out of network domain 104"'a and/or 104"'b. If so, monitor/regulator 102"' takes appropriate action to warn and/or "stop" the undesirable/inappropriate network traffics from being sourced out of network domain 104"'a and/or 104b"'. Accordingly, systems disposed

inside network domain 104" are protected from exploitation in providing involuntary assistance to DOS attacks against other systems, or their owners ~~be~~ are at least alerted of their exploitations.--

Replace the paragraph beginning at page 16, line 7, in the specification as originally filed, with the following rewritten paragraph:

--As the earlier described embodiment, monitor/regulator 102"' periodically requests characteristic data of network traffics 106"' routed, except instead of making such requests of only routing device or device(s) of one network domain, monitor/regulator 102"' makes the periodic requests with all the boundary routing devices, such as routing device 114"'a as well as routing device 114"'b, of all network domains 104"'a and 104"'b.--

Replace the paragraph beginning at page 16, line 13, in the specification as originally filed, with the following rewritten paragraph:

--Similarly, when monitor/regulator 102''' makes its determination on whether undesirable/inappropriate network traffics are being sourced out of network domain 104"'a and/or 104"'b, monitor/regulator 102''' takes all the data received into consideration. That is, when analyzing the data received from routing device 114"'a of network domain 114"'a, monitor/regulator 102''' adds or otherwise factors into consideration the data received from other routing devices of the same or other network domains, such as routing device 114"'b of network domain 104"'b. Likewise, when analyzing the data received from routing device 114"'b of network domain 104"'b, monitor/regulator 102''' adds or otherwise factors into consideration the data received from other routing devices of the same or other network domains, such as routing device 114"'a of network domain 104"'a. As described earlier, the data may be any one of the example data enumerated above, aggregated or at individual flow level.--

Replace the paragraph beginning at page 17, line 1, in the specification as originally filed, with the following rewritten paragraph:

--By aggregating or otherwise ~~takes~~ taking into consideration characteristic data of network traffics sourced out of other network domains, monitor/regulator 102"' is made even more sensitive, and ~~be~~ is able to detect undesirable/inappropriate network

traffics being sourced out network domain 104"'a and/or network domain 104"'b, even though the decision metrics may not be exceeded at the individual routing devices and/or the individual network domains. For example, upon determining that undesirable network traffics are being sourced out of one domain, the threshold criteria for concluding that undesirable network traffics are being sourced out of another domain may be "lowered", as the probability of erroneously concluding that a domain is also being exploited to support the attack is substantially lower, given it has already been determined another domain is being exploited to source an attack. Accordingly, under this embodiment, the detection and prevention can advantageously leverage on information learned and/or determinations made for other domains.--

Replace the paragraph beginning at page 17, line 15, in the specification as originally filed, with the following rewritten paragraph:

--In one embodiment, monitor/regulator 102"' warns the owner(s) of the systems of network domain 104"' of the detection. For the illustrated embodiment, monitor/regulator 102"' determines the regulation instructions, if needed, separately for the different routing devices of the different network domains. That is, monitor/regulator 102"' determines separate regulation instructions, if any, for the different routing devices of the different network domains. In an alternate embodiment, monitor/regulator 102"' may determine the regulation instructions collectively, and have the regulation instructions be applied to all routing devices of all network domains uniformly.--